GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Newsletter

NOTIZIARIO SETTIMANALE
ANNO XV
WWW.GARANTEPRIVACY.IT

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NEWSLETTER N. 370 del 1° marzo 2013

Sull'autobus una telecamera che registra gli incidenti

Sì del Garante alla registrazioni delle immagini, ma senza audio

Sì alle telecamere sugli autobus per registrare gli incidenti, ma no alle registrazioni audio. Il Garante per la privacy ha autorizzato [doc. web n. 2257616] la società concessionaria del servizio di trasporto pubblico locale di Bergamo e di altri ventisette comuni dell'area urbana ad installare sul parabrezza anteriore dei propri veicoli un dispositivo che in caso di incidenti consente di registrare le immagini della sede stradale e quelle della zona interna del mezzo di trasporto, nei venti secondi precedenti e successivi all'evento.

Con l'impiego di questo sistema di rilevazione - che non riprende il conducente - la società tramviaria intende agevolare la ricostruzione dei sinistri in cui sono coinvolti gli autobus, salvaguardare quindi i beni aziendali e indirettamente accrescere la sicurezza di utenti e dipendenti.

Nel dare il via libera l'Autorità ha chiesto però ulteriori garanzie. Il sistema non dovrà registrare le conversazioni a bordo dell'autobus e i passeggeri dovranno essere informati della sua presenza anche attraverso cartelli con disegni stilizzati, ben visibili sui mezzi di trasporto.

La società inoltre, dovrà rendere interamente "trasparenti" i trattamenti di dati personali effettuati portandoli a conoscenza dei dipendenti e in particolare dei conducenti dei veicoli. Un'informativa dettagliata rivolta alla collettività dovrà essere pubblicata anche sul sito web, nelle registrazioni, infatti, oltre i passeggeri potrebbero essere ripresi i conducenti di altri veicoli o altre persone presenti sulla sede stradale.

Alla società infine, è stato ordinato di predisporre meccanismi di integrale cancellazione automatica delle informazioni allo scadere del termine (24 mesi) previsto dal codice civile per far valere eventuali pretese di risarcimento danni prodotti dalla circolazione dei veicoli e di adottare adeguate misure di sicurezza per preservare l'integrità dei dati e prevenire accessi abusivi da parte di personale non autorizzato.

Medicina a distanza: defibrillatori a prova di privacy

Tecnologia Rfid impiantata in pazienti cardiopatici

Sì all'uso di defibrillatori a distanza per pazienti cardiopatici, ma nel rispetto della privacy degli interessati. Lo ha stabilito il Garante con un provvedimento di rilevanza generale [doc. web n. 2276103] con il quale ha prescritto precise e rigorose misure a protezione dei dati dei pazienti a un'Azienda ospedaliera lombarda e a una società francese produttrice di apparecchiature medicali che avevano chiesto all'Autorità di potersi avvalere di un sistema a radiofrequenza (Rfid) per il monitoraggio remoto dei pazienti mediante defibrillatori cardiaci impiantati sotto pelle. L'uso di sistemi a radiofrequenza destinati all'impianto sottocutaneo attraverso "etichette intelligenti" solleva, infatti, questioni estremamente delicate e presenta rischi potenziali, sia per la sicurezza dei dati personali trattati, particolarmente delicati, sia sotto il profilo della salute.

Il sistema che intende adottare l'Azienda ospedaliera prevede l'inserimento nel microchip, inserito nel defibrillatore impiantato sotto la cute del paziente, di dati clinici. Tali informazioni sono trasmesse in modalità wireless ad un monitor installato in casa del paziente e dal monitor al server situato presso l'azienda ospedaliera mediante linea telefonica. Scopo del sistema è quello di consentire ai medici di monitorare costantemente via web il paziente, evitando la tradizionale visita ospedaliera, rilevare eventuali anomalie cardiache e nel caso effettuare con tempestività la defibrillazione.

L'Autorità ha ribadito che per fornire il servizio è necessario il consenso informato dei pazienti. Ma ha soprattutto stabilito che il paziente dovrà poter ottenere in modo agevole la disattivazione sia del sistema remoto sia del funzionamento dell'etichetta Rfid contenuta nel dispositivo impiantato.

Una delle criticità rilevate dal Garante riguarda il fatto che la società produttrice del sistema, designata dall'ospedale quale responsabile del trattamento, si avvale di operatori esterni in subappalto, a cui sono delegate alcune attività di manutenzione e sicurezza del sistema. Considerata la delicatezza dei dati ai quali gli operatori esterni possono avere accesso, il Garante ha disposto che la società possa avvalersi di terzi soltanto previo accordo con l'ospedale. I soggetti terzi che accedono ai dati devono essere sottoposti ai medesimi obblighi a cui è tenuta la società fornitrice come responsabile del trattamento.

Qualora i dati clinici memorizzati nel sistema vengano messi a disposizione anche di altri operatori sanitari che abbiano in cura il paziente, questi ultimi, quali titolari autonomi del trattamento, sono obbligati a raccogliere preventivamente il libero e specifico consenso del paziente.

Il Garante ha prescritto che tutte le operazioni di trattamento dei dati effettuate dall'Azienda ospedaliera, dal fornitore del servizio o dagli operatori esterni coinvolti debbano essere registrate.

Le informazioni sugli accessi devono essere fornite al paziente su sua richiesta.

L'Autorità ha inoltre prescritto rigorose misure di sicurezza a protezione dei dati sanitari: in particolare, credenziali di autenticazione del sistema remoto e strumenti di gestione delle utenze che prevedano la possibilità di effettuare controlli degli accessi con l'attivazione di sistemi di alert.

Ai sindacati niente dati nominativi sul lavoro straordinario

Le pubbliche amministrazioni, in assenza di disposizioni normative o di specifiche clausole contenute in contratti collettivi, non possono comunicare le ore di straordinario svolte da un dipendente indicando anche il nome e il cognome dello stesso. Le comunicazioni vanno fatte in forma anonima o aggregata. Lo ha stabilito [doc. web n. 2288474] il Garante privacy che ha imposto al Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia di interrompere la trasmissione alle organizzazioni sindacali dei dati relativi alle ore di straordinario effettuate da un commissario di polizia penitenziaria. L'interessato, non iscritto ad alcun sindacato, aveva lamentato la comunicazione in forma nominativa, alle organizzazioni sindacali del comparto sicurezza, del prospetto concernente le prestazioni di lavoro straordinario da lui effettuate e le relative competenze. Ritenendo violate le norme sulla privacy, aveva chiesto che il Dipartimento cessasse tale trattamento illecito dei dati.

Non avendo ottenuto riscontro, si era è rivolto dunque all'Autorità chiedendo che i suoi dati personali non venissero né trasmessi alle OO.SS., né affissi e quindi diffusi in locali comuni.

L'istruttoria condotta dal Garante ha messo in luce come nel caso in questione non esistono né disposizioni normative né disposizioni contenute in accordi sindacali di settore che legittimino la trasmissione in forma nominativa di informazioni relative alle ore di straordinario svolto dai dipendenti dell'Amministrazione penitenziaria: l'Accordo Nazionale quadro per il personale del Corpo di polizia penitenziaria, risalente al 2004, prevede infatti solo la comunicazione in forma anonima dei prospetti delle prestazioni di lavoro straordinario.

Nella sua decisione l'Autorità ha richiamato inoltre quanto previsto dalle Linee guida del Garante del 14 giugno 2007 (doc. web n. 1417809), sul trattamento dei dati personali nel rapporto di lavoro pubblico, le quali stabiliscono che l'amministrazione pubblica può fornire alle organizzazioni sindacali dati numerici e aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili".

Nell'accogliere dunque il ricorso dell'interessato e ritendendo pertanto illecito il trattamento effettuato dall'amministrazione penitenziaria, l'Autorità ha disposto il blocco dell'ulteriore comunicazione dei dati del dipendente addebitando le spese del ricorso al Ministero.

Sì alla televigilanza, ma senza violare i diritti dei lavoratori

Bloccato impianto video di un' importante catena commerciale

Il servizio di televigilanza, con scopo di anti-taccheggio e anti-rapina, non deve consentire forme di controllo a distanza dei lavoratori. Gli esercenti devono segnalare adeguatamente la presenza di telecamere e affidare la gestione del servizio a guardie giurate.

Queste le indicazioni del Garante [doc. web n. 2291893] che, in seguito all'attività ispettiva condotta dalla Questura di Genova, ha bloccato il trattamento dei dati effettuato tramite il sistema di videosorveglianza installato in un esercizio di un'importante catena commerciale.

Dalle verifiche effettuate è emerso che la società aveva violato in più punti l'accordo che era stato sottoscritto con i sindacati per l'installazione delle telecamere sul luogo di lavoro. Una videocamera, ad esempio, invece che essere utilizzata per finalità di sicurezza, inquadrava il sistema di rilevazione degli accessi dei dipendenti, consentendo quindi ï in contrasto con quanto sottoscritto dall'azienda e con lo stesso Statuto dei lavoratori - il controllo a distanza dei lavoratori. Le immagini registrate risultavano poi accessibili con modalità diverse da quelle concordate. Non erano in regola neppure i cartelli con l'informativa semplificata utilizzati per segnalare la presenza dell'impianto di videosorveglianza: non solo non contenevano tutte le informazioni necessarie, ma erano in numero esiguo e, a volte, collocati in posizione non chiaramente visibile (ad es. alle spalle di un espositore). Dai riscontri della Questura è emerso, inoltre, che l'impianto di videosorveglianza era stato affidato in gestione a un consorzio di ditte esterne che utilizzava per il servizio personale non qualificato. Chi effettuava il controllo delle immagini era, infatti, privo della licenza prefettizia di "guardia particolare giurata", necessaria per poter svolgere funzioni anti-rapina e anti-taccheggio, e non era stato designato incaricato del trattamento dei dati personali.

Il Garante della privacy ha imposto all'esercente di provvedere a sanare tutte le violazioni riscontrate e ha bloccato il trattamento dei dati effettuato attraverso il sistema di videosorveglianza. Ha anche trasmesso copia degli atti e del provvedimento all'autorità giudiziaria al fine di valutare gli eventuali illeciti penali commessi.

L'ATTIVITÁ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÚ

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

- Il Garante scrive a WhatsApp: come utilizzate i dati degli utenti italiani? (Comunicato del 27 febbraio 2013)
- Cookie e privacy: c'è tempo fino al 19 marzo per partecipare alla consultazione pubblica del Garante (Comunicato del 28 febbario 2013)
- Dichiarazione di Antonello Soro. L'azione contro Google tutela cittadini e imprese UE (28 febbraio 2013)

NEWSLETTER
del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).
Direttore responsabile: Baldo Meo.
Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.
Tel: 06.69677.2752 - Fax: 06.69677.3755
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it*